UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/791,414	03/03/2004	Jing Xiang	NRT.0124US	2562

21906 7590 04/04/2011

TROP, PRUNER & HU, P.C.
1616 S. VOSS ROAD, SUITE 750
HOUSTON, TX 77057-2631

EXAMINER	
TABOR, AMARE F	
ART UNIT	PAPER NUMBER
2434	

MAIL DATE	DELIVERY MODE
04/04/2011	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/791,414	XIANG ET AL.	
	Examiner	Art Unit	
	AMARE TABOR	2434	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 January 2011*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *10-12,14,17 and 20-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *10-12,14,17 and 20-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to **Amendments** and **REMARKS** filed on 01/14/2011.

2. Independent claim 12 is amended; and claims 26-28 are new.

3. **Claims 10-12, 14, 17 and 20-28** are pending.

35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 10-12, 14, 17 and 20-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Joseph et al. (US 6,966,003 B1, hereafter "**Joseph**") in view of Bahl et al. (US 7,020,464 B2, hereafter "**Bahl**").

As per Claim10, Joseph teaches:

A method for maintaining secure network connections, the method comprising: duplicating [see for example, col.2, lines 24-61], at a third network element, a security association associated with a secure network connection between a first network element and a second network element [see FIG.1: where first (12), second (22), third (22') & (fourth=30) are disclosed], and in response to detecting failure of the second network element [Fig.2b; claims 8, 11, 18 and 24], replacing the second network

element with the third network element in the secure network connection with the first network element [see FIG.1 (network device 22' is back-up device) and FIG.2B; and for example, col.4, lines 58-67], wherein the secure network connection between the first network element and the third network element is based on the duplicated security association [see step 118 in FIG.2B].

Joseph fails to disclose wherein a lookup of the security association associated with the secure network connection is not dependent on any destination address; however, in analogous art, **Bahl** teaches a lookup of the security association associated with the secure network connection is not dependent on any destination address [see FIGS.4A-6: SA is not changed when mobile node changes old to new address (e.g., col.11, lines 45-47)]. Therefore, it would have been obvious to a person having ordinary skill in the art at the time of applicant's invention was made to modify the system of **Joseph** by incorporating the teaching of **Bahl** in order to provide transparent session continuity [see at least abstract of **Bahl**].

As per Claims 11 and 20, Joseph in view of Bahl teaches:

The method according to claim 10 further comprising sending at least one secure message from the third network element to the first network element to notify the first network element that the secure network connection will be taken over by the third network element [see abstract and 'second communication' 34 in FIG.1 of **Joseph**]; and during life of the secure network connection between the first and second network

elements, the third network element receiving information relating to the security association of the secure network connection from the second network element [see abstract and FIGS.1 and 2B of **Joseph**].

As per Claims 21 and 23, Joseph teaches:

The method of claim 10, the second and third network elements are security servers [see FIG.1; and for example, col.3, lines 31-34]. **Joseph** does not teach the first network element as a mobile client. However, **Bahl** teaches a first network element as a mobile client [see 'mobile host' 70 in FIG.1]. Therefore, it would have been obvious to a person having ordinary skill in the art at the time of applicant's invention was made to modify the system of **Joseph** by incorporating the mobile host of **Bahl** in order to handle network communications between mobile devices [see at least col.1, 9-13 of **Bahl**].

As per Claim 26, Joseph in view of Bahl,

The method of claim 10, wherein replacing the second network element with the third network element in the secure network connection comprises the third network element sending a notification to the first network element that the third network element is taking over the secure network connection [see FIG.1 (network device 22' is back-up device) and FIG.2B; and for example, col.4, lines 58-67].

As per Claim 27, Joseph in view of Bahl teaches:

The method of claim 10, further comprising: after replacing the second network element within the third network element in the secure network connection, the third network element communicating with the first network element without the third network element re-establishing another connection with the first network element [see Figure 2b; claims 8, 11, 18 and 24: a secondary secure connection replaces the first, but no any other connection is re-established].

As per Claim 12, Joseph teaches:

A method for maintaining secure network connections, the method comprising: configuring a plurality of security gateways (such that a lookup of security associations is not dependent on any destination address) [see abstract and FIGS.1 and 3-4: where network devices to be configured are disclosed]; sharing a security association among the plurality of security gateways [see abstract and FIG.2B and 3-4; and for example, col.2, lines 24-61]; a first of the security gateways detecting failure of a second of the security gateways involved in a secure connection with a network device [Fig.2b; claims 8, 18 and 24], wherein the secure network connection is associated with the security association [see step 118 in FIG.2B]; and in response to detecting the failure, the first security gateway sending a message to the network device that the first security gateway is taking over the secure network connection [see FIG.1 (network device 22' is back-up device) and FIG.2B; and for example, col.4, lines 58-67].

Joseph fails to disclose wherein a lookup of the security association associated with the secure network connection is not dependent on any destination address; however, in analogous art, **Bahl** teaches a lookup of the security association associated with the secure network connection is not dependent on any destination address [see FIGS.4A-6: SA is not changed when mobile node changes old to new address (e.g., col.11, lines 45-47)]. Therefore, it would have been obvious to a person having ordinary skill in the art at the time of applicant's invention was made to modify the system of **Joseph** by incorporating the teaching of **Bahl** in order to provide transparent session continuity [see at least abstract of **Bahl**].

As per Claim 25, Joseph in view of Bahl teaches:

The method of claim 12, wherein sharing the security association comprises sharing an IPsec security association among the plurality of security gateways [see FIGS.3-4 and step 204 in FIG.5A of **Joseph**: where security information (IPsec) is disclosed].

As per Claims 14 and 22, Joseph teaches:

A first security server comprising: a transceiver to receive information relating to at least one security association of a secure network connection between a (mobile) client and a second security server [see abstract; FIGS.1 and 3-4, connection status based on SA is transmitted]; and a processor module to: monitor operation of the second security server [see abstract and FIGS.1 and 3-4, network connection is

monitored for failure]; in response to detecting failure of the second security server [Fig.2b; claims 8, 11, 18 and 24], send a message to the (mobile) client that the first security server is taking over the secure network connection [see FIG.1 (network device 22' is back-up device) and FIG.2B; and for example, col.4, lines 58-67]; and communicate with the (mobile) client using the at least one security association over the secure network connection between the first security server and the (mobile) client [see step 118 in FIG.2B].

Joseph fails to disclose mobile client and a lookup of the security association associated with the secure network connection is not dependent on any destination address; however, in analogous art, **Bahl** teaches a mobile client [see 'mobile host' 70 in FIG.1] and lookup of the security association associated with the secure network connection is not dependent on any destination address [see FIGS.4A-6: SA is not changed when mobile node changes old to new address (e.g., col.11, lines 45-47)]. Therefore, it would have been obvious to a person having ordinary skill in the art at the time of applicant's invention was made to modify the system of **Joseph** by incorporating the teaching of **Bahl** in order to provide transparent session continuity of mobile communications [see at least abstract of **Bahl**].

As per Claims 17, Joseph in view of Bahl teaches:

The first security server according to claim 22, wherein communications between the mobile client [see 'mobile host' 70 in FIG.1] and the first security server are based

on a security architecture for the internet protocol (IPsec) [see FIGS.3-4 and step 204 in FIG.5A of **Joseph**: where security information (IPsec) is disclosed].

The same motivation used with respect to claim 22 above is used, because the secondary reference is applied to map the same limitation (i.e., mobile client).

As per Claim 24, Joseph in view of Bahl teaches:

The first security server of claim 22, wherein information relating to the at least one security association is duplicated at the first and second security servers [see for example, col.2, lines 24-61 of **Joseph**].

As per Claim 28, Joseph in view of Bahl, and further in view of Xxx teaches:

The first security server of claim 22, wherein the processor module is configured to communicate with the mobile client after taking over the secure network connection without re-establishing a new connection [see Figure 2b; claims 8, 11, 18 and 24: a secondary secure connection replaces the first, but no any other connection is re-established].

Response to Arguments

5. Applicant's arguments filed have been fully considered but they are not persuasive.

Applicant argues "…in Joseph, rather than replacing the second network element with the third element in the secure network connection (which was between the first network element and the second network element), Joseph discloses the establishment

of a new connection between the first and third network devices in response to failure of the first communication between the first and second network devices" [REM, p.6]. Examiner respectfully disagrees and notes that, A) Joseph discloses "…a first secure communication being established between the first and second network devices, and a second secure communication being established between the first and third network devices" [abstract]. B) In Joseph "the second secure communication (which is between the first and the third network device) has the same (or duplicated) security association as the first secure communication" [see abstract], which maps to the claimed "secured connection between the first network element and the third network element is based on duplicated security association". Finally, C) when the first communication fails, Joseph does not establish a new connection as applicant argues above, but the system of Joseph **replaces** "the first [secure] communication **with** the second [secure] communication when the first communication fails" [see Figure 2b; claims 8, 11, 18 and 24].

Conclusion

6. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to **AMARE TABOR** whose telephone number is (571)270-3155. The examiner can normally be reached on Mon-Fri 8:00a.m. to 5:00p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, **KAMBIZ ZAND** can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Amare Tabor/
Examiner, Art Unit 2434

/Jacob Lipman/
Primary Examiner, Art Unit 2434